REMARKS/ARGUMENTS

Claims 1, 3-16, and 18-20 are pending in this case (claims 2 and 17 were previously canceled). In the pending Office Action mailed March 9, 2007 designated "Final", the Examiner rejected all of the pending claims under 35 U.S.C. § 103 (a) over the combination of Kasmirsky (US Publication No. 2004/0193740) in view of Zahavi (US Publication No. 2005/0086646) and Nilsson (US Publication No. 2005/0188229). In this Amendment After Final, amendments to the independent claims (claims 1, 10, 13, 16) are presented to recite that the claimed system and method are directed to storing data management rule information with a data file to specify both retention and relocation of the data file. The dependent claims have been amended as needed for consistency with the amended independent claims. It is submitted that the claims, upon entry of the amendments, are patentable over the art of record. No new matter has been added.

Accompanying this Amendment After Final is a Request for Continued Examination. Entry of the amendment in the RCE case and action on the merits are requested.

The Claim Amendments

All of the independent claims, as amended by this Amendment After Final, recite storing data management rule information with a data file to specify retention and relocation of the data file. This is described in the specification at, for example, paragraph [0012] at page 3, lines 8-9, and paragraph [0052] at page 10, lines 3-4. See also Figure 6 and paragraph 0052 (header of data file includes data management rules including retention and relocation information).

Claim 1 as amended recites a storage system that includes a host that stores data management rule information with a data file to determine how to protect and relocate the data file, a first storage subsystem to store the data file, and a data protection server and a data relocation server to take appropriate action for retention and relocation, respectively, as follows:

> a host configured to receive a data file from a client, the host including a data management rule set program that is operable to associate data

management rule information to the data file received from the client and determine how to protect and relocate the data file;

a first storage subsystem configured to receive and store the data file from the host, the storage system including a storage controller and a plurality of storage volumes, wherein the data management rule information is stored in a header of the data file;

a data protection server including a data protection management program that cooperates with the first storage subsystem to protect the data file stored in the first storage subsystem in accordance with the management rule information, the data protection server looking up the data management rule information in the header of the data file to determine action to protect the data file; and

a data relocation server that controls relocation of the data file from the first storage subsystem to another storage subsystem.

Claim 10 recites a management server that includes the data rule management information for data file retention and relocation through a first data management program of the server:

a first management program to attach data management rule information to a data file to be stored in a storage subsystem of the storage system, the data management rule information relating to a retention period and to relocation information of the data file.

Claim 13 recites a management server that includes a first management program that looks up data management rule information relating to data file retention and relocation:

a first management program operable to access a header of a data file to look up data management rule information inserted in the header and manage the data file according to the data management rule information inserted in the header, the data management rule information relating to a retention period and to relocation instructions of the data file.

Claim 16 recites a method for data file management that includes attaching data management rule information relating to retention and to relocation of the data file, the method including operations of:

attaching data management rule information to the data file;

storing the data file and the data management rule information at a first storage location in a first storage subsystem, the data management rule information relating to retention and to relocation information of the data file.

By keeping data management rule information for data retention and relocation information with a data file, the present invention permits data management policy to be shared across multiple services and servers of a data system. See paragraphs [0010] and [0011] of the specification.

The Section 103 Rejection Over the Combination of Kasmirsky, Zahavi, and Nilsson

It is submitted that the combination of Kasmirsky, Zahavi, and Nilsson does not render obvious the claims as amended herein.

In the pending Office Action, the Examiner rejected claims 1, 3-16, and 18-20 under 35 U.S.C. § 103(a) as being unpatentable over Kasmirsky in view of Zahazi and Nilsson. Applicant asserts that the Office Action does not provide a *prima facie* case for obviousness and asserts that the claims as amended are patentable over the proposed combination.

In accordance with M.P.E.P. § 2143, to establish a *prima facie* case of obviousness, three basic criteria must be met: (1) there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings; (2) there must be a reasonable expectation of success; (3) the prior art reference (or references when combined) must teach or suggest all the claim limitations.

1. No teaching or suggestion of all claim limitations

As noted above, all the independent claims recite storing data management rule information with a data file to specify retention and relocation of the data file. In one embodiment, the system includes both a protection server and a relocation server (Figure 4A and 4B). Maintaining retention and relocation information for stored data files permits the present invention to support multiple data solutions from multiple vendors (see Figure 2 and Figure 4A and 4B of the application, and corresponding specification at pages 6-9). That is, the claimed invention makes it possible to share data retention and data relocation information of data files across data systems. The prior art does not show this.

Kasmirsky makes no mention of sharing retention and relocation information across systems. Rather, the stored data files are under control of a database manager and there is

no need for storing relocation information in a file data header. More particularly, as shown in Fig. 3, Kasmirsky provides a storage system in which data is received from sources 52 and is analyzed by a format analyzer 62[1] to produce metadata that is characteristic of the data. The metadata is stored into a database 82 according to a rule engine 84, which specifies a storage option for the received data. The data storage is managed by a database manager 82. See paragraphs [0054]-[0056] of Kasmirsky. That is, the stored data is accessed via the database manager (see paragraph 0057, lines 10-16).

Zahavi describes a system to monitor and manage performance of a plurality of storage components, such as disk storage arrays 20, within a storage system (see Fig. 2 and paragraph [0031] of Zahavi). Again, a single data manager is presented (see Fig. 2 and Fig. 3) and there is no mention of sharing retention and relocation information across systems.

Nilsson describes a protection server that maintains integrity of personal data. In Nilsson, access to the protected personal data is limited through the solitary protection server, working with an intermediate proxy server to restrict requests for information. This is in direct contrast to sharing of information across systems. There is no discussion in Nilsson of managing data retention and relocating data across systems.

Thus, no combination of the cited references could provide the cited feature of data management rule information stored in a data file header for retention (protection) and relocation of the data file. Therefore, the proposed combination does not teach or suggest all the claim limitations of the rejected claims, and there is no *prima facie* case for the obviousness rejection.

2. No Suggestion for the Proposed Combination

Kasmirsky relates to a storage system in which data is received from outside sources producing data of different file types. The data is analyzed to produce metadata that is characteristic of the data content. The metadata is used in conjunction with a rule engine at the time of data store to determine data storage options (see paragraph [0056] of Kasmirsky).

[1] The format analyzer is incorrectly identified as "82" in Fig. 3 but is correctly referenced in the specification.

Zahavi produces data relating to the performance of disk storage arrays and stores the performance metrics in ASCII text files. For example, software agents 30 invoke system calls to collect data about the disk storage array 20 performance, including configuration information such as number of volumes and disks (see paragraph [0032]). The collected data comprises an ASCII text file with system performance metrics over predetermined intervals, such as hourly, daily, weekly, or monthly (paragraph [0044]-[0047]). Each stored file includes a header block that contains a description of the system configuration that generated the metrics and the order of the performance interval data contained within the data file (see paragraph [0048] and [0049]). It is apparent that the Zahavi header data is provided for the purpose of facilitating configuration review of the system that produced the data file metrics, through a Performance Review component (see paragraph [0075] of Zahavi).

There would be no reason for combining the Kasmirsky metadata technique for determining data storage options (based on file content of multiple file types) with the Zahavi header data technique that stores system configuration information in a data header of a corresponding ASCII data file (that contains performance metrics for the system configured per the data header). Moreover, it is asserted that there would be no reason to combine either of these two systems (Kasmirsky and Zahavi) with the personal data security system of Nilsson, who is concerned with maintaining the integrity of end user personal profile data through a protection server.

Therefore, there is no suggestion or motivation for combining Kasmirsky, Zahavi, and Nilsson, absent impermissible hindsight reconstruction, and there is no *prima facie* case for the obviousness rejection.

3. No reasonable expectation of success

Kasmirsky receives data files of different types from multiple sources and produces metadata in accordance with the various data types such that the metadata indicates storage options for the data type. Zahavi collects system performance statistics and produces data of a common file type (ASCII) for storage, with header data that indicates the system configuration that produced the ASCII performance data. Kasmirsky uses metadata that reflects

the content of the associated file, whereas Zahavi uses header data that reflects a system configuration that produced the data. It is submitted that one would not know how to combine these two systems without using the present disclosure as a guide.

Similarly, the protection server of Nilsson is used for restricting access to personal profile data through an intermediate proxy server, and it is not clear how one would combine such a server with the metadata-controlled storage options system of Kasmirsky and the configuration-indicating file header information of Zahavi.

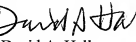
Therefore, there is no reasonable expectation of successfully combining Kasmirsky, Zahavi, and Nilsson, and there is no *prima facie* case for the obviousness rejection. Evidence showing there is no reasonable expectation of success in combining may support a conclusion of nonobviousness (In re Rinehart, 531 F.2d 1048, 189 U.S.P.Q. 143 (C.C.P.A. 1976)).

Applicant submits that the Office Action does not provide a *prima facie* case for obviousness of claims 1, 3-16, and 18-20 in view of Kasmirsky, Zahavi, and Nilsson, and therefore claims 1, 3-16, and 18-20 are patentable over the references.

CONCLUSION

In view of the foregoing, Applicant asserts that the claims, as amended, are patentable over the cited references and are not properly rejected on the grounds and over the art currently of record. An allowance of all claims now pending in this application is respectfully requested.

Respectfully submitted,



David A. Hall
Reg. No. 32,233

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 858-350-6100 Fax: 415-576-0300
Attachments
DAH:dah
61074827 v1